IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

E.R., a Minor, through her Guardian, L.H., **K.M.**, a Minor, through her Guardian, C.M., **D.M.**, a minor, through her Guardian, D.H., **L.B.**, a minor, by and through his or her guardian, Molly Janik, **H.S.**, a Minor, through her Guardian, J.S., each individually and on behalf of all others similarly situated, Plaintiffs, v. TIKTOK, INC. and BYTEDANCE, INC., Defendants.	No. 1:20-cv-02810 **CONSOLIDATED ACTION** Hon. John Z. Lee **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, E.R., a minor, by and through her Guardian L.H., K.M., a minor, by and through her Guardian C.M., D.M., a minor, by and through her Guardian D.H, L.B., a minor, by and through his or her Guardian Molly Janik, and H.S., a minor by and through her Guardian J.S., each individually and on behalf of a Class of all others similarly situated as defined below (the "Class"), by and through their attorneys, bring the following Consolidated Class Action Complaint ("Complaint") pursuant to Rule 23 of the Federal Rules of Civil Procedure, against Defendants TikTok, Inc. ("TikTok") and ByteDance, Inc. ("ByteDance") (collectively the "Defendants"). They allege the following based upon personal knowledge as to themselves and their own actions, and, as to all other matters, allege, upon information and belief and investigation of their counsel, as follows:

NATURE OF THE ACTION

1. Defendants operate the social media platform TikTok (formerly Musical.ly), one of the most popular entertainment apps for mobile devices in the United States and the world.

2. The TikTok app allows users to create and share 15-second videos - typically of people doing activities such as dancing, lip-syncing, and stunts - and boasts a fanbase of more than **two billion** worldwide, the vast majority of whom are teenagers and children.[1]

3. TikTok's owner, ByteDance, was founded in 2012 and remains based in Beijing, China. ByteDance is well known as a hit app factory that has spent the last decade using technologies such as artificial intelligence and facial recognition.[2] TikTok currently has approximately 2.4 million active daily users, many of whom are minors. This action seeks to ensure that the privacy of Illinois minors who use TikTok is adequately protected.

4. Plaintiffs and class members have particular concerns here given TikTok's reported connections to the Chinese government, which have very recently come under close public scrutiny. Several U.S. Senators have formally requested that the Intelligence Community conduct an assessment of the national security risks posed by TikTok.[3] Recognizing the serious ongoing threat posed by TikTok, prominent U.S. Senators wrote to the FTC on May 29, 2020 that, "[f]aced

---

[1] Paige Leskin, *TikTok Surpasses 2 Billion Downloads and Sets a Record for App Installs in a Single Quarter*, Business Insider (April 30, 2020), available at https://www.businessinsider.com/tiktok-app-2-billion-downloads-record-setting-q1-sensor-tower-2020-4 (last accessed June 12, 2020); *see also* Maryam Moshin, *10 TikTok Statistics That You Need To Know in 2020*, Oberlo (February 17, 2020), *available at* https://www.oberlo.com/blog/tiktok-statistics (last accessed June 12, 2020).

[2] Shelly Banjo, *Worries That TikTok Is A Threat To National Security Have Merit,* at https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit (last accessed June 12, 2020).

[3] *See* Letter to Acting Director Maguire, October 23, 2019, attached hereto as **Exhibit A**

with ***compelling*** evidence that this wildly popular social media platform is ***blatantly flouting binding U.S. privacy rules***, the FTC should move swiftly to launch an investigation and forcefully hold violators accountable for their conduct."[4]

5. Because of data privacy concerns, some U.S. military branches have even banned the use of the app on government-issued phones. Republican Senator Josh Hawley called for a total ban on the use of the app across the United States.[5] Reddit CEO and co-founder Steve Huffman called TikTok "fundamentally parasitic" due to privacy concerns.[6]

6. In fact, the Department of Defense recently expressed concern over TikTok's "popularity with Western Users, and its ability to convey location, image and ***biometric data*** to its Chinese parent company, which is legally unable to refuse to share data to the Chinese Government," going so far as to issue an internal memo to encourage its employees to avoid installing the app.[7]

7. Plaintiffs bring this class action against TikTok for violations of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS §14/1, *et seq.* BIPA prohibits, among other things,

---

[4] *See* Letter to the Federal Trade Commission Chairman and Commissioners, May 29, 2020, attached hereto as **Exhibit B** (emphasis added).

[5] TJ McCue, *Is TikTok Raiding Your Privacy in 2020? Here Is How To Stop It*, *available at* https://www.forbes.com/sites/tjmccue/2020/02/13/is-tiktok-raiding-your-privacy-in-2020-here-is-how-to-stop-it/#1e34f6b569c8 (last accessed June 12, 2020).

[6] Chaim Gartenberg, *Reddit CEO Says TikTOk Is "Fundamentally Parasitic," Cites Privacy Concerns*, *available at* https://www.theverge.com/2020/2/27/21155845/reddit-ceo-steve-huffman-tiktok-privacy-concerns-spyware-fingerprinting-tracking-users (last accessed June 12, 2020).

[7] Jason Aten, *The Department of Defense Is Warning People Not to Use TikTok Over National Security Concerns*, Forbes (January 9, 2020) (quoting internal memo), *available at* https://www.inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html (last accessed June 12, 2020) (emphasis added).

private entities from collecting, capturing, obtaining, disclosing, redisclosing, disseminating or profiting from the biometric identifiers or information of an individual without providing written notice and without obtaining a written release from the impacted individual or his or her authorized representative. BIPA also requires private entities in possession of biometric identifiers to adopt retention and destruction policies and to take measures to prevent the release of that information.

8. As alleged in detail below, Defendants, through the TikTok app, collected, captured, obtained, stored and, upon information and belief, disclosed and otherwise disseminated Illinois resident minor TikTok users' biometric information.

9. Various features of the TikTok app, including its alleged "Face Swap" feature, automatically scan and collect user's biometric identifiers, ***even for users who have not created accounts***.[8]

10. TikTok accesses its users' data for various purposes, including tracking users by age, gender, location, operating system, and interest in order to attract marketing and ad sales. By collecting and filtering this user data, TikTok offers a sophisticated targeted ad and marketing platform that allows its ad clientele to hone into their target demographics with shocking precision.[9]

---

[8] *See* Peter Suciu, *TikTok's Deepfakes Just The Latest Security Issue For The Video Sharing App*, Forbes (January 7, 2020), *available at* https://www.forbes.com/sites/petersuciu/2020/01/07/tiktoks-deepfakes-just-the-latest-security-issue-for-the-video-sharing-app/#707ead6970a2 (last accessed June 12, 2020). *See also* Jesse Hirsh, *New Platform, Old Problems: How TikTok Recreates the Regulatory Challenge that Came Before It, Canadian Centre for International Governance Innovation* (May 18, 2020) *available at* https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it (last accessed June 12, 2020).

[9] *See* Maria Mellor, *Why is TikTok creating filter bubble based on your race?,* Wired (February 28, 2020), a*vailable at* https://www.wired.co.uk/article/tiktok-filter-bubbles (last accessed June 12, 2020).

11. Defendants engaged in this conduct: (a) without adequately informing the impacted minors, including minor Plaintiffs and their parents or lawful guardians, and the minor members of the proposed class (the "Class Members") and their parents or lawful guardians, that biometric identifiers were being collected, captured, obtained, disclosed, redisclosed or otherwise disseminated; (b) without informing the impacted minors, and their parents or lawful guardians, in writing of the purpose of the collection, capture, obtainment, disclosure, redisclosure and dissemination of the biometric identifiers and information; and (c) without seeking and obtaining consent or written releases from such impacted minors and their parents or lawful guardians.

12. As the Illinois General Assembly has found and both the Illinois Supreme Court and Seventh Circuit Court of Appeals have confirmed, the harm to Plaintiffs and Class Members as a result of the BIPA violations alleged herein has already occurred.

13. Further, as businesses worldwide compete to develop ever more advanced facial recognition technology, the race for data imperils the privacy of individuals everywhere. Public policy in Illinois provides that given the risks of unwanted data collection and disclosure, citizens need the power to make decisions about the fate of their unique biometric identifiers and information. Defendants' actions robbed Plaintiffs and Class Members of that power.

14. Defendants' conduct is particularly brazen given that it is specifically directed at minors and involves the misuse of their biometric information without seeking parental consent.

15. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of $5,000 per BIPA violation, or, alternatively, if Defendants acted negligently, $1,000 per BIPA violation, along with attorneys' fees and costs; (b) disgorgement of Defendants' ill-gotten gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i) barring Defendants from any further use of minors' biometric identifiers and information; (ii) barring Defendants from

continuing to collect, capture, obtain, disclose, redisclose, disseminate and profit from Plaintiffs' and Class Members' biometric identifiers and information; (iii) requiring Defendants to delete and destroy all biometric identifiers and information in their possession, custody and control; and (iv) requiring Defendants to claw back the biometric identifiers and information from any third parties to whom Defendants disclosed, redisclosed or disseminated it.

PARTIES

16. At relevant times, Plaintiff E.R., a minor, was and remains an Illinois resident. Plaintiff E.R.'s Guardian, L.H. was also, at relevant times, and is through the date of this filing an Illinois resident. Defendants performed facial geometric scans of Plaintiff E.R. through Plaintiff E.R.'s use of the TikTok app, while Plaintiff E.R. resided in Illinois. Like tens of thousands or more other Class Members in Illinois, Plaintiff E.R. downloaded the TikTok app in Illinois and uploaded videos to the app in Illinois.

17. At relevant times, Plaintiff K.M., a minor, was and remains an Illinois resident. Plaintiff K.M.'s Guardian, C.M. was also, at relevant times, and is through the date of this filing an Illinois resident. Defendants performed facial geometric scans of Plaintiff K.M. through Plaintiff K.M.'s use of the TikTok app, while Plaintiff K.M. resided in Illinois. Like tens of thousands or more other Class Members in Illinois, Plaintiff K.M. downloaded the TikTok app in Illinois and uploaded videos to the app in Illinois.

18. At relevant times, Plaintiff D.M., a minor, was and remains an Illinois resident. Plaintiff D.M.'s Guardian, D.H. was also, at relevant times, and is through the date of this filing an Illinois resident. Defendants performed facial geometric scans of Plaintiff D.M. through Plaintiff D.M.'s use of the TikTok app, while Plaintiff D.M. resided in Illinois. Like tens of

thousands or more other Class Members in Illinois, Plaintiff D.M. downloaded the TikTok app in Illinois and uploaded videos to the app in Illinois.

19. At relevant times, Plaintiff L.B., a minor, was and remains an Illinois resident. Plaintiff L.B.'s Guardian, Molly Janik, was also, at relevant times, and is through the date of this filing an Illinois resident. Defendants performed facial geometric scans of Plaintiff L.B. through Plaintiff L.B.'s use of the TikTok app, while Plaintiff L.B. resided in Illinois. Like tens of thousands or more other Class Members in Illinois, Plaintiff L.B. downloaded the TikTok app in Illinois and uploaded videos to the app in Illinois.

20. At relevant times, Plaintiff H.S., a minor, was and remains an Illinois resident. Plaintiff H.S.'s Guardian, J.S. was also, at relevant times, and is through the date of this filing an Illinois resident. Defendants performed facial geometric scans of Plaintiff H.S. through Plaintiff H.S.'s use of the TikTok app, while Plaintiff H.S. resided in Illinois. Like tens of thousands or more other Class Members in Illinois, Plaintiff H.S. downloaded the TikTok app in Illinois and uploaded videos to the app in Illinois.

21. Defendant TikTok, Inc. is a California corporation with its principal place of business in Culver City, California. TikTok, Inc. has a registered agent in Illinois.

22. Defendant ByteDance, Inc. is a Delaware corporation with its principal place of business in Palo Alto, California. ByteDance, Inc. has a registered agent in Illinois.

23. Based on Plaintiffs' investigation and the evidence obtained concerning the direct culpability of the U.S. based Defendants, Plaintiffs do not name, at this time, the following related foreign entities: Musical.ly n/k/a TikTok, Ltd. (a Cayman Islands corporation with its principal place of business in Shanghai, China), Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance") (a privately held company headquartered in Beijing, China) or ByteDance Co., Ltd.

(the owner of Bejing ByteDance headquartered in Beijing, China) (together, the "Chinese Entities"). Plaintiffs reserve their rights to seek discovery from Defendants concerning the involvement of the Chinese Entities and to name them as defendants in the future should that discovery or further investigation reveal an appropriate jurisdictional basis for doing so.

JURISDICTION AND VENUE

24. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class. Because it is estimated that the Class will have thousands of members and Defendants' intentional and reckless violations of BIPA are punishable by statutory damages of $5,000 per violation, the amount in controversy is well in excess of $5,000,000.

25. This Court has personal jurisdiction over Defendants because Defendants used and disseminated data derived directly from Illinois-based TikTok users and exposed residents of Illinois to ongoing privacy risks within Illinois based on the collection, capture, obtainment, disclosure, redisclosure and dissemination of their biometric identifiers and information. Furthermore, many of the images Defendants used for their unlawful collection, capture and obtainment of biometric identifiers and information were created in Illinois, uploaded from Illinois, and/or managed via Illinois-based user accounts, computers, and mobile devices. Because of the scope and magnitude of Defendants' conduct, Defendants knew that their collection, capture, obtainment, disclosure, redisclosure and dissemination of impacted individuals' biometric identifiers and information would injure Illinois residents and citizens. Defendants knew or had reason to know that collecting, capturing, obtaining, disclosing, redisclosing and disseminating

Illinois citizens' and residents' biometric identifiers and information without providing the requisite notice or obtaining the requisite releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their biometric identifiers and information via their Illinois-managed devices and exposed minors in Illinois to potential surveillance and other privacy harms as they went about their lives within the state.

26. Furthermore, through the TikTok app, Defendants actively collect information harvested from the Illinois-based devices of Illinois residents, including "location information" based on users' "SIM card and/or IP address."[10]

27. Defendants use this harvested information to "provide [users] with location-based services, such as advertising and other personalized content" directed toward Illinois.[11]

28. Defendants' deliberate gathering of Illinois users' personally identifiable information is intentionally targeted toward Illinois residents, including Plaintiffs and the Class, and constitutes purposeful activity directed at devices and individuals in Illinois.

29. Indeed, Defendants attract advertisers by touting the TikTok's app's ability to target users by, among other things, location, stating that "[i]t has never been easier to reach potential customers by precisely targeting your audience. Using TikTok Ads, you can target your audience

[10] https://www.tiktok.com/legal/privacy-policy?lang=en (last accessed June 12, 2020).

[11] *Id.*

by gender, location, age, interests, and other unique variables."[12] TikTok expressly targets its advertisements by State, including, upon information and belief, within Illinois.[13]

30. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims alleged herein occurred in Illinois. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendants.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

31. BIPA seeks to safeguard individuals' biometric identifiers and information.

32. Biometric identifiers include a scan of an individual's face geometry or voiceprint. 740 ILCS § 14/10.

33. Biometric information is "any information . . . based on an individual's biometric identifier used to identify an individual." 740 ILCS § 14/10.

34. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

35. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because

[12] https://ads.tiktok.com/help/article?aid=6667447877242978309 (last accessed June 12, 2020).

[13] https://ads.tiktok.com/help/article?aid=6721969269619294213 (last accessed June 12, 2020) (describing "Ad Targeting" by "state/province").

suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

36. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

37. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

38. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

39. Biometric identifiers include retina and iris scans, fingerprints and handprints, and – most importantly here – facial geometry and voiceprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

40. BIPA establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

41. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

42. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at a heightened risk for identity theft and left without any recourse.

43. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

44. Plaintiffs, like the Illinois legislature, recognize how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendants' Unlawful Conduct

45. ByteDance, Inc., the parent company of TikTok, Inc., first launched the TikTok app (then known as "Douyin") in China in September 2016. The app ultimately became available in the United States in August 2018 following a merger between TikTok and Shanghai-based social media platform Musical.ly.[14] While TikTok and Douyin are similar to each other and essentially the same app, they run on separate servers to comply with Chinese censorship restrictions.

46. In 2019, Douyin introduced the "in-video" search function, which allows users to filter for individuals using facial recognition. This function "allows users to highlight and search

[14] In November of 2019, the New York Times reported that the United States government had opened a national security review of the 2017 acquisition of Musical.ly, the American predecessor of TikTok, by the Chinese company ByteDance based on concerns that data from TikTok was being shared with China. *See* Jack Nicas, Mike Isaac, and Ana Swanson, *TikTok Said to Be Under National Security Review*, The New York Times (November 1, 2019), *available at* https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html (last accessed June 12, 2020).

the platform for the face of a person within a video."[15] While this function is not active in TikTok, Douyin users in China, or elsewhere, can perform in-video searches for Illinois citizens.

47. In Illinois, and in direct violation of BIPA, the TikTok app's proprietary facial recognition technology scans every video uploaded to the app for faces, extracts geometric data relating to the unique points and contours (*i.e.,* biometric identifiers) of each face, and then uses that data to create and store a template of each face - all without ever informing anyone of these practices.

48. To accomplish this end, Defendants implemented the same artificial intelligence tool that is used in the Douyin app in order to automatically perform facial scans. This technology permits users to superimpose images onto their face or to use various "filters" that alter, distort, or enhance their facial features.

49. This technology, known as Deepfake, extracts biometrics in order to "superimpose your face onto any video, or any picture, or anything" says Richard Jackson, Cybersecurity Division Chief at Fort Knox. [16]

50. Similarly, the TikTok app also applies proprietary biometric recognition technology to scan every video uploaded to the app for voiceprints (*i.e.,* biometric identifiers), extracting similar data points to create and store voiceprints of each user - all without ever informing anyone of these practices.

---

[15] *See* Jessica Rapp, *In-video search: A new opportunity for influencer marketing on Douyin?*, PR Week (November 6, 2019), *available at* https://www.prweek.com/article/1664878/in-video-search-new-opportunity-influencer-marketing-douyin (last accessed June 12, 2020).

[16] Eric Pilgic, *Army Cybersecurity: Social media platforms offer children exciting, frightening environments*, U.S. Army (January 22, 2020), *available at* https://www.army.mil/article/231909/army_cybersecurity_social_media_platforms_offer_children_exciting_frightening_environments (last accessed June 12, 2020).

51. As clearly stated in TikTok's Privacy Policy, TikTok's user data is subsequently transferred and shared with servers located outside the United States including backup servers located in Singapore.[17] Further, prior to TikTok's 2019 privacy changes, American user data was shared, stored, and processed in the "United States of America, Singapore, Japan or [] China."[18]

52. In addition, Defendants profit from the use of individuals' biometric identifiers. Defendants extract users' biometric identifiers in order to precisely categorize target audiences for advertisers, thus maintaining a competitive advantage over other social media advertising platforms. In effect, Defendants have surreptitiously created an immense commercial database, consisting of millions, if not billions, of users' data - including Plaintiffs' unique and personally identifiable biometric identifiers - that can be used for further commercial advantage and other harmful purposes.[19]

53. The TikTok app also allows users to sign into the apps through Facebook, Google, and Twitter – in turn allowing Defendants access to biometric identifiers stored in each individual's social media accounts.

---

[17] *See* TikTok Privacy Policy as of January 1, 2020, *available at* https://www.tiktok.com/legal/privacy-policy?lang=en (last accessed June 12, 2020).

[18] Helen Ehrlich, TikTok is Scamming People & Stealing Information, Affinity (November 4, 2018), *available at* http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/ (last accessed June 12, 2020).

[19] *See* Reindhart Krause, *TikTok Raises Profile As Digital Ad Rival to Snap, Facebook, Google,* Investor's Business Daily (May 18, 2020) (discussing TikTok's rising popularity and stating that "big brands in digital advertising – such as restaurant chain Chipotle Mexican Grill (CMG), cosmetics firm Elf Beauty (ELF), Walmart (WMT) and Ralph Lauren (RL) — have experimented with ads on TikTok.") *available at* https://www.investors.com/news/technology/tik-tok-video-app-digital-advertising/ (last accessed June 12, 2020).

54. By utilizing these biometric databases, TikTok maintains a competitive advantage over other social media apps and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling users' biometric data established by BIPA.[20]

55. In addition, former Musical.ly users who accessed the app prior to its consolidation with the current TikTok app have no idea to whom Musical.ly disclosed their biometric data or what third parties may have accessed their biometric data as a consequence of this consolidation.

56. Having become ubiquitous among teenagers and children alike, TikTok puts ***millions*** of children's biometric information at risk, without the consent or knowledge of their parents or lawful guardians.

57. In collecting, capturing and otherwise obtaining the biometric identifiers and information of Plaintiffs and Class Members and, upon information and belief, subsequently disclosing, redisclosing and otherwise disseminating those biometric identifiers and information to other related corporate entities – all without providing the requisite notice, obtaining the requisite releases or satisfying any of BIPA's other provisions that would excuse it from BIPA's mandates – Defendants violated BIPA.

58. In further violation of BIPA, as a private entity in possession of Plaintiffs' and Class Members' biometric identifiers and information, Defendants failed to adopt or make available to the public a retention schedule or guidelines for permanently destroying such biometric identifiers and information once the initial purpose for collecting them had or has been satisfied.

---

[20] *See* Lauren Strapagiel, *This Researcher's Observation Shows the Uncomfortable Bias of TikTok's Algorithm*, Buzzfeed News (February 26, 2020), *available at* https://www.buzzfeednews.com/article/laurenstrapagiel/tiktok-algorithim-racial-bias (last accessed June 12, 2020).

59. Defendants' violations of BIPA were intentional and reckless or, in the alternative, negligent.

III. Allegations Related to Plaintiffs

60. Each Plaintiff, an Illinois minor, separately downloaded the TikTok app onto their mobile device(s). Initially, Plaintiffs were not required to disclose information about their age, nor were they required to enter a written release before receiving a TikTok account.

61. Each Plaintiff uploaded and posted numerous videos to TikTok, which included images of their faces, and/or their faces have appeared in other users' uploaded videos. Each Plaintiff has been subject to, either through their own videos or the videos of others in which they have appeared, TikTok's face sticker, face filter, face tracker lens, and voiceprint filter technologies.

62. Through these videos, Defendants have collected and stored Plaintiffs' unique biometric identifiers or biometric information. Defendants have subsequently disclosed and/or disseminated these biometric identifiers or biometric information to third parties, including out of state servers which store the biometric information.

63. Defendants shared Plaintiffs' biometric identifiers without their or their legal guardians' knowledge, or consent.

64. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' multiple violations of BIPA alleged herein.

65. No amount of time or money can compensate Plaintiffs if their biometric identifiers are compromised by the lax procedures through which Defendants captured, stored, used, and disseminated their and other similarly-situated individuals' biometrics. Moreover, Plaintiffs would not have provided their biometric identifiers to Defendants, and their legal guardian would not

have consented to their use of TikTok, had they known that Defendants would retain such information for an indefinite period of time without consent.

66. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp*., 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

67. As Plaintiffs are not required to allege or prove actual damages in order to state a claim under BIPA, they seek statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

IV. Plaintiffs' Claims Are Not Subject to Arbitration

68. Certain of TikTok's Terms of Use purport to require users to submit to arbitration and to waive all rights to pursue legal proceedings against Defendants through the class action device. These terms are invalid and unenforceable against minors, including Plaintiffs and the Class.

69. Under Illinois law, a minor is without legal capacity to enter into a contract and thus is legally incapable of contracting in the first place. Because Plaintiffs and Class members are all minors, Defendants cannot enforce any purported arbitration and/or class action waiver against Plaintiffs or the Class because no agreement was ever formed in the first place.

70. Furthermore, while Defendants attempt to surreptitiously secure minor users' "consent" to TikTok's Terms of Use – which such users cannot legally provide -- Defendants do not make any attempt to secure the consent of parents or lawful-guardians.

71. Defendants have not obtained consent from the parents or lawful guardians of Class Members for their accounts.

72. Defendants fail to make reasonable efforts to ensure that a parent or lawful guardian of Class Members receives direct notice of their practices regarding the collection, use, or disclosure of personal information.

73. Defendants do not at any point contact the parents or lawful guardians of Class Members to give them notice and do not even ask for contact information for the parents or lawful guardians of Class Members.

74. Thus, Defendants have no means of obtaining verifiable parental consent, or the consent of any lawful guardian, before any collection, use, or disclosure of the personal information of Class Members, nor do Defendants obtain verifiable parental consent to any alleged arbitration or class action waiver provisions.

CLASS ALLEGATIONS

75. Plaintiffs bring this action individually and as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following Class for which Plaintiffs seek certification:

> **All Illinois residents under the age of 18 who had their facial geometry, voiceprint, or other biometric identifier collected, captured, received, or otherwise obtained, maintained, stored or disclosed by Defendants during the applicable statutory period.**

76. Excluded from the Class are: (a) Defendants; (b) any parent, affiliate or subsidiary of Defendants; (c) any entity in which Defendants have a controlling interest; (d) any of Defendants' officers or directors; or (e) any successor or assign of Defendants. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

77. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

78. **Numerosity.** While the exact number of Class Members is not known at this time, Defendants collected, captured, obtained, disclosed, redisclosed and otherwise disseminated biometric identifiers and information from hundreds of millions of users, and Plaintiffs estimate the total number of Class Members to be, at least, in the tens of thousands. Consistent with Rule 23(a)(1), the proposed Class is therefore so numerous that joinder of all members is impracticable. Class Members may be identified through objective means, including objective data available to Defendants regarding their user data. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice

79. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the proposed Class. Common questions include, but are not limited to, the following:

a. Whether Defendants collected, captured and otherwise obtained the biometric identifiers and information of Plaintiffs and Class Members;

b. Whether Defendants possessed the biometric identifiers and information of Plaintiffs and Class Members;

c. Whether Defendants disclosed, redisclosed and otherwise disseminated the biometric identifiers and information of Plaintiffs and Class Members;

d. Whether Defendants profited from the biometric identifiers and information of Plaintiffs and Class Members;

e. Whether Defendants provided the notice required by BIPA before collecting, capturing, obtaining, disclosing, redisclosing and otherwise disseminating the biometric identifiers and information of Plaintiffs and Class Members;

f. Whether Defendants obtained enforceable written releases from Plaintiffs and Class Members or their authorized representatives before collecting, capturing, obtaining, disclosing, redisclosing and otherwise disseminating the biometric identifiers and information or Plaintiffs and Class Members;

g. Whether Defendants had in place – and disclosed to the public – the written retention and destruction policies required by BIPA while in possession of Plaintiffs' and Class Members' biometric identifiers and information;

h. Whether Defendants protected Plaintiffs' and Class Members' biometric identifiers and information from disclosure using the reasonable standard of care within Defendants' industry and in a manner that was the same as or more protective than the manner in which Defendants protects other confidential and sensitive information;

i. Whether Plaintiffs and Class Members suffered damages as a proximate result of Defendants; and

j. Whether Plaintiffs and Class Members are entitled to damages, equitable relief and other relief.

80. **Typicality.** Plaintiffs' claims are typical of the claims of the Class because Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the

same practices alleged herein. Plaintiffs have no interests to advance adverse to the interests of the other members of the proposed Class.

81. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class and have retained as counsel attorneys experienced in class actions and complex litigation.

82. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not be of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of a single adjudication, economy of scale and comprehensive supervision by a single court.

83. In the alternative, the proposed Class may be certified because:

a. The prosecution of separate actions by each individual member of the proposed Class would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendants;

b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class Members or which would substantially impair their ability to protect their interests; and

c. Defendants acted or refused to act on grounds generally applicable to the proposed Class, thereby making final and injunctive relief appropriate with respect to members of the proposed Class.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

84. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

85. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

86. Defendants fail to comply with these BIPA mandates.

87. Defendants qualify as "private entities" under BIPA. *See* 740 ILCS § 14/10.

88. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their facial geometry and/or voiceprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

89. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

90. Defendants failed to publish a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

91. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and have not and will not destroy Plaintiffs' or the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the app.

92. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

93. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

94. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release

executed by the subject of the biometric identifier or biometric information…" 740 ILCS § 14/15(b) (emphasis added).

95. Defendants fail to comply with these BIPA mandates.

96. Defendants are "private entities" under BIPA. *See* 740 ILCS § 14/10.

97. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their facial geometry and/or voiceprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

98. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

99. Defendants systematically and automatically collected, used, stored and disseminated Plaintiffs' and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS § 14/15(b)(3).

100. Defendants did not inform Plaintiffs and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, used and disseminated, nor did Defendants inform Plaintiffs and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, used, and disseminated as required by 740 ILCS § 14/15(b)(1)-(2).

101. By collecting, storing, and using Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, Defendants violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

102. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by

requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

103. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

104. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS § 14/15(d)(1).

105. Defendants fail to comply with this BIPA mandate.

106. Defendants qualify as "private entities" under BIPA. *See* 740 ILCS § 14/10.

107. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their facial geometry and/or voiceprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

108. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

109. Defendants systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS § 14/15(d)(1).

110. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, Defendants violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

111. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiffs, E.R., a minor, by and through her Guardian L.H., K.M., a minor, by and through her Guardian C.M., D.M., a minor, by and through her Guardian D.H., L.B., a minor, by and through his or her Guardian Molly Janik, and H.S., a minor by and through her Guardian J.S., respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as Class representatives and appointing undersigned counsel as Class Counsel;

B. Declaring that Defendants' actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendants' actions, as set forth above, were intentional and/or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including an Order requiring Defendants to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiffs and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Date: June 12, 2020

Respectfully Submitted,

/s/ Katrina Carroll
Katrina Carroll
kcarroll@carlsonlynch.com
Kyle A. Shamberg
kshamberg@ carlsonlynch.com
Nicholas R. Lange
nlange@carlsonlynch.com
111 W. Washington Street, Suite 1240
Chicago, IL 60602
Telephone: (312) 750-1265

Douglas A. Millen
Brian M. Hogan
FREED KANNER LONDON & MILLEN LLC
2201 Waukegan Road, Suite 130
Bannockburn, Illinois 60015
Tel.: (224) 632-4500
Fax: (224) 632-4521
dmillen@fklmlaw.com
bhogan@fklmlaw.com

Jonathan M. Jagher
Kimberly A. Justice
FREED KANNER LONDON & MILLEN LLC

923 Fayette St.
Conshohocken, PA 19428
Tel.: (610) 234-6487
Fax: (224) 632-4521
jjagher@fklmlaw.com
kjustice@fklmlaw.com

Jennifer W. Sprengel
Daniel O. Herrera
Nickolas J. Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
150 S. Wacker, Suite 3000
Chicago, Illinois 60606
Telephone: 312-782-4880
Facsimile: 318-782-4485
jsprengel@caffertyclobes.com
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Joseph G. Sauder
Joseph B. Kenney
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (610) 200-0580
Fax: (610) 421-1326
jgs@sstriallawyers.com
jbk@sstriallawyers.com

Richard R. Gordon
Gordon Law Offices, Ltd.
111 West Washington Street
Suite 1240
Chicago, Illinois 60602
Tel: (312) 332-5200
Fax: (312) 242-4966
rrg@gordonlawchicago.com

James B. Zouras
Ryan F. Stephan
Andrew C. Ficzko
Megan E. Shannon
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza,
Suite 2150

Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
aficzko@stephanzouras.com
mshannon@stephanzouras.com

Erik H. Langeland (*pro hac vice forthcoming*)
733 Third Avenue, 15th Floor
New York, N.Y. 10017
(212) 354-6270
elangeland@langelandlaw.com

Jon A. Tostrud (*pro hac vice forthcoming*)
TOSTRUD LAW GROUP, P.C.
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
(310) 278-2600
jtostrud@tostrudlaw.com

Counsel for Plaintiffs and the Putative Class